

UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE COURT

2013 NOV -5 PM 4:42

In re Motions for Declaratory)
Judgment to Disclose Aggregate)
Data Regarding FISA Orders)
and Directives)

Case Nos. Misc. 13-03, 13-04, 13-05, 13-06,
and 13-07

LEEANN FLYNN HALL
CLERK OF COURT

**AMICUS CURIAE BRIEF OF APPLE INC. IN SUPPORT OF PROVIDERS' MOTIONS
FOR DECLARATORY JUDGMENT**

Apple Inc. ("Apple") submits this *amicus* brief in support of motions for declaratory judgment filed by Google Inc., Microsoft Corporation, Yahoo! Inc., Facebook, Inc., and LinkedIn Corporation seeking permission to publish the aggregate numbers of national security demands made on them and the number of users or accounts affected by those requests. As with these providers, and fellow *amicus curiae* Dropbox, Inc., the Government has told Apple that it may not publish the aggregate number of national security demands, if any, it may receive. Apple concurs with the previously submitted filings of movants and *amici* and describes herein the interest of Apple and its customers in the motions that have been filed. In addition, Apple provides additional analysis as to why the Government's position both (i) lacks any statutory basis and (ii) violates the First Amendment right of Apple and others to provide the public and its customers with important information on an issue that has been the subject of intense political debate and public concern.¹

STATEMENT OF INTEREST AND FACTUAL BACKGROUND

Amicus Apple is one of the world's largest designers, manufacturers, and sellers of mobile communication and media devices, personal computers, and portable digital music players and also sells a variety of related software and services. Its notable products and services

¹ Nothing in this filing is intended to confirm or deny that Apple has received any order or orders issued by this Court under the Foreign Intelligence Surveillance Act or the FISA Amendments Act.

include the iPhone, iPad, Mac, iPod, Apple TV, iOS and OS X operating systems, iCloud, and a variety of accessory, service, and support offerings. In the first nine months of its 2013 fiscal year, it sold 173.5 million iPads and iPhones and has sold over 700 million such devices in its lifetime.² These Apple devices are increasingly linked to its cloud service, iCloud. iCloud stores email, music, photos, applications, contacts, calendars, and documents which can be accessed by Apple mobile devices and Mac and Windows-based personal computers. Access to iCloud (with storage limitations) is free for all Apple customers that purchase devices using its iOS operating system for mobile devices, or Mac computers that use OS X. Apple now has 350 million iCloud customers worldwide. As stated in its November 5, 2013 Report on Government Information Requests (attached as Exhibit 1), Apple believes that its “customers have a right to understand how their personal information is handled” and considers it to be Apple’s “responsibility to provide them with the best privacy protections available.” Ex. 1 at 1.

In June of 2013, articles in major newspapers reported erroneously that Apple and other technology companies had enabled an alleged National Security Agency program known as “PRISM” to tap into providers’ central servers. *E.g.*, Glenn Greenwald and Ewen MacAskill, *The NSA Prism Program Taps in to User Data of Apple, Google and Others*, *The Guardian* (June 6, 2013), available at <http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data>; Barton Gellman and Laura Poitras, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, *The Washington Post* (June 6, 2013), available at <http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845->

² Apple Inc., Quarterly Report (Form 10-Q), at 27 (July 24, 2013), available at <http://www.sec.gov/Archives/edgar/data/320193/000119312513300670/d552802d10q.htm>; Press Release, Apple Inc., iOS 7 with Completely Redesigned User Interface & Great New Features Available September 18 (Sept. 10, 2013), available at <http://www.apple.com/pr/library/2013/09/10iOS-7-With-Completely-Redesigned-User-Interface-Great-New-Features-Available-September-18.html>.

d970ccb04497_story.html. To correct the misinformation in these reports and address customer concerns, on June 16, 2013 Apple issued its Commitment to Customer Privacy. *See Apple's Commitment to Customer Privacy*, Apple (June 16, 2013), *available at* www.apple.com/apples-commitment-to-customer-privacy. In that statement, Apple explained that it does “not provide any government agency with direct access to our servers, and any government agency requesting customer content must get a court order.” *Id.*

Apple additionally sought permission from the FBI to disclose the aggregate number of national security requests that it received and the number of accounts affected by each applicable national security authority (e.g., NSL, FISA, and Section 702 of FISA). In a phone conversation on June 15, 2013, and then by letter of June 17, 2013, the General Counsel of the FBI refused the request. Instead, Apple was informed that it could only provide data that aggregated

all the legal process it received for intervals of six months, beginning with the period ending May 31, 2013, from any and all government entities in the United States (including local, state, and federal, and including criminal and national security-related requests) into bands of 1000, starting at zero, and which you may break down into one or both of the following two categories: the number of requests and the number of user accounts for which data was requested.

Exhibit 2, Letter from Andrew Weissmann, Gen. Counsel, Fed. Bureau of Investigation, to Jane Horvath, Dir. of Global Privacy, Apple Inc. (June 17, 2013) (emphasis added). Thus, the FBI required Apple to group the receipt of national security requests with requests from police investigating robberies and other crimes, searching for missing children, or hoping to prevent a suicide. And even aggregated in this way, Apple must use ranges of 1,000 rather than disclose a precise number.

The FBI did not designate its letter or any of its contents as classified at any level. The FBI also did not assert that the information Apple sought to disclose was classified. The FBI did not even mention any issue of classified information as pertinent to the issues here.

In its letter, the FBI instead discussed the FISA statute as the relevant issue. Even on that issue, the FBI did not identify anything in the law that authorizes the Government to prohibit disclosure of the aggregate number of national security requests received by Apple. Instead, the Bureau's letter portrayed its decision as an exercise of its discretion not to enforce the statute against Apple specifically. *Id.* at 1 (“[W]e do not intend to seek enforcement of the non-disclosure provisions associated with any legal process, including FISA orders, in connection with the aggregate data described below . . . [and this] position is an exercise of FBI discretion in light of current circumstances and the precise contours of this letter.”). It further reserved the right to reach a different conclusion as to other companies and/or to restrict further Apple's ability to disclose even this limited information upon notice to Apple.

As a result of these restrictions, in its most recent report Apple was able to disclose to the public and its customers only that it has received 1,000-2,000 requests for user account information affecting 2,000-3,000 user accounts from all federal, state, and local law-enforcement agencies combined. *Ex. 1* at 3. The report further states that actual data were disclosed in 0-1,000 instances. *Id.* From Apple's perspective, as well as the perspective of its customers and the public as a whole, this limited disclosure does not contribute effectively to the debate over the Government's national security systems and (as discussed *infra*) is unnecessary to protect national security. By design, it combines the aggregate data that are of the greatest and most timely public concern, and the greatest concern to Apple and its customers, with other unrelated aggregate data in a deliberate attempt to reduce public knowledge as to the activities of the Government.

ARGUMENT

I. THE GOVERNMENT HAS NO LEGAL AUTHORITY TO PROHIBIT THE DISCLOSURE OF THE AGGREGATE NUMBER OF NATIONAL SECURITY REQUESTS.

Apple concurs with movants that nothing in FISA or any other law prohibits providers from disclosing aggregate information about the number of demands they receive by individual national security authority (e.g., NSL, FISA, and Section 702 of FISA). Under FISA, a particular order may direct the recipient to furnish necessary assistance for the particular surveillance “in such a manner as will protect its secrecy.” 50 U.S.C. § 1805(c)(2)(B) (2013); *see also id.* § 1824(c)(2)(B) (same requirement for a physical search where the target is a foreign power or the agent of a foreign power); *id.* § 1881a(h)(1)(A) (same requirement for a request to an electronic communications service provider for persons located outside the United States); *id.* § 1881b(c)(5)(B) (same requirement where the target is a United States person located outside the United States). These provisions are designed to protect the secrecy of particular orders in order to preserve the integrity of ongoing investigations. They are not designed to preclude companies from reporting aggregate data. Nothing in FISA’s text or legislative history suggests that the Act prohibits a recipient of a FISA order from confirming (or denying) the basic fact that it has (or has not) received nondescript legal process under FISA, or from disclosing the aggregate number of requests it has received.

FISA generally requires providers to maintain any records they generate as a result of these requests “under security procedures approved by the Attorney General and the Director of National Intelligence.” *Id.* § 1805(c)(2)(C); *see also id.* § 1881a(h)(1)(B). These provisions have the same purpose – i.e., protecting target-specific data – and do not impose a ban on the disclosure of aggregate numbers of requests a provider receives. 50 U.S.C. § 1807 even requires the Attorney General to publish aggregate data across providers, and the Attorney General has

previously released such reports to the public.³ *Id.* § 1807. FISA thus supports the disclosure of aggregate data.

The Government's response to Apple's request confirms the absence of any legal support for its position. As discussed above, the letter from the FBI's General Counsel at no point claims that Apple's proposed disclosures would cover classified information. Nor does the letter identify any legal authority supporting its position. Instead, it asserts that the FBI will not "enforce" the nondisclosure provisions against Apple as an exercise of its "discretion," if Apple's disclosure is limited in the manner prescribed by the FBI. *See* Ex. 2. It is thus fair to assume that the FBI is well aware that there is no legal authority for its position but is using its non-enforcement discretion as a way of creating a de facto licensing system for aggregate data disclosure that has no foundation in law.

The Government's recent filing does not point to anything in FISA that prohibits disclosure of the relevant material. It relies only on provisions allowing it to "protect the secrecy of *the acquisition*" and "records concerning *the acquisition or aid furnished*." Response of the United States to Motions for Declaratory Judgment by Google Inc., Microsoft Corporation, Yahoo Inc., Facebook, Inc., and LinkedIn Corporation ("Gov't Resp.") at 13 (internal citations and quotation marks omitted) (emphasis added). Disclosure of the aggregate number of requests received, however, would not reveal anything or provide any "records" about any particular "acquisition" or "the acquisition or aid furnished."

³ *See* Letter from Peter J. Kadzik, Principal Deputy Assistant Attorney Gen., U.S. Dep't of Justice, to Harry Reid, Majority Leader, U.S. Senate (Apr. 30, 2013), *available at* http://www.justice.gov/nsd/foia/foia_library/2012fisa-ltr.pdf (noting that (1) during 2012, the Government made 1,856 applications to the FISC for authority to conduct electronic surveillance and/or physical searches for foreign intelligence purposes; and (2) the FISC did not deny any applications in whole or in part).

The Government asserts that there would be a “wide range of damaging disclosures” from the proposed disclosure here. *Id.* at 14. Notably, however, the Government fails to identify a single one other than a vague reference to topics “from the nature of surveillance targets to their general locations.” *Id.* at 4. These examples are not at all clear, and the Government notably fails to provide any elaboration to its public filing on this point as to how aggregate data could, for example, disclose anything about surveillance targets much less their “nature” or “location.”

To the extent, however, that the Government is suggesting that the proffered interpretation would allow damaging disclosures about particular requests, that is not the case. FISA permits the Government to prevent the disclosure of information about particular requests even if the disclosure does not identify a target by name. It does not, however, prohibit the release of the aggregate number of requests received and accounts affected by individual national security authority (e.g., NSL, FISA, or Section 702 of FISA) where no details are provided about any individual request.

The Government’s filing also claims, for the first time, that all of the data the providers seek to disclose are classified. *See id.* at 5-6. This argument does nothing to alter the fact that the Government has failed to identify anything in FISA (the subject of the Court’s jurisdiction) that prohibits the disclosure of the aggregate number of FISA process received and accounts affected by individual national security authority (e.g., NSL, FISA, or Section 702 of FISA). Further, as described above, at no point in the FBI’s initial response to the providers did the Bureau suggest that a disclosure aggregating received national security legal process by individual national security authority (e.g., NSL, FISA, or Section 702 of FISA) would be classified. It is thus implausible for the Government now to claim that the aggregate number of

legal contacts providers may receive under each individual national security authority and accounts affected thereby is itself classified.

Further, Apple, along with certain other providers, has sought to report only the total number of national security legal process received and accounts affected in the aggregate by individual national security authority (e.g., NSL, FISA, or Section 702 of FISA). That basic information cannot be considered “properly classified” – given the wide variety of tools available to the Government under FISA and other factors discussed in the next section, such an aggregate disclosure of legal process under the Act would not offer would-be adversaries any useful information regarding the Government’s intelligence sources or methods.

II. THE BLANKET BAN ON DISCLOSING THE AGGREGATE NUMBER OF NATIONAL SECURITY REQUESTS VIOLATES THE FIRST AMENDMENT BECAUSE IT IS NOT NECESSARY TO PROTECT NATIONAL SECURITY.

The legal standard that governs this dispute is straightforward, and the Government does not deny it. Under the First Amendment, content-based restrictions such as the restrictions at issue here are subject to strict scrutiny and are thus “presumptively invalid.” *United States v. Stevens*, 559 U.S. 460, 468 (2010) (content-based restrictions are “‘presumptively invalid,’ and the Government bears the burden to rebut that presumption”) (quoting *United States v. Playboy Ent. Grp., Inc.*, 529 U.S. 803, 817 (2000)). Further, because the Government has prohibited providers from speaking about aggregate data without first obtaining the Government’s permission, the restriction is a prior restraint and presumptively invalid for that reason as well. *Am. Freedom Defense Initiative v. WMATA*, 898 F. Supp. 2d 73, 79 (D.D.C. 2012) (a prior restraint bears “a heavy presumption against its constitutional validity”) (quoting *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70 (1963)); see *Neb. Press Ass’n v. Stuart*, 427 U.S. 539, 559 (1976) (“[P]rior restraints on speech and publication are the most serious and the least tolerable infringement on First Amendment rights.”). Moreover, “speech on public issues” such as the

Government’s surveillance program “occupies the highest rung of the hierarchy of First Amendment values, and is entitled to special protection.” *See Snyder v. Phelps*, 131 S. Ct. 1207, 1215 (2011) (quoting *Connick v. Myers*, 461 U.S. 138, 145 (1983)); *Mills v. Alabama*, 384 U.S. 214, 218 (1966) (“[T]here is practically universal agreement that a major purpose of [the First] Amendment was to protect the free discussion of governmental affairs.”).

To survive strict scrutiny, a restriction must, at a minimum, be “necessary to serve a compelling state interest” and “narrowly drawn to achieve that end.” *Am. Freedom Defense Initiative*, 898 F. Supp. 2d at 80 (quoting *Perry Educ. Ass’n v. Perry Local Educators’ Ass’n*, 460 U.S. 37, 45 (1983)); *see also United States v. Alvarez*, 132 S. Ct. 2537, 2549, 2551 (2012) (the “First Amendment requires that the Government’s chosen restriction on the speech at issue be ‘actually necessary’ to achieve its interest” and that such a “restriction must be the ‘least restrictive means among available, effective alternatives’”) (quoting *Ashcroft v. Am. Civil Liberties Union*, 542 U.S. 656, 666 (2004)).

As various courts have recognized, this is a “demanding standard” that few restrictions survive. *See Brown v. Ent. Merchs. Ass’n*, 131 S. Ct. 2729, 2738 (2011) (quoting *Playboy Ent. Grp., Inc.*, 529 U.S. at 818); *Am. Freedom Defense Initiative*, 898 F. Supp. 2d at 80-81 (there “is no doubt that content-based restrictions can rarely pass constitutional review” and neither party “points to a case concerning a content-based restriction where the Supreme Court concluded that the government had a compelling interest *and* the restriction could be approved because it was sufficiently narrowly tailored”).

Courts vigorously enforce the narrow tailoring requirement in both the national security and non-national security contexts. *See Al Haramain Islamic Found., Inc. v. U.S. Dep’t of the Treasury*, 686 F.3d 965, 997-1001 (9th Cir. 2012) (restrictions on providing aid to terrorists

violated the First Amendment based on the failure of the Government to establish that the restrictions were “narrowly tailored to advance the concededly compelling government interest of preventing terrorism”); *Doe v. Mukasey*, 549 F.3d 861, 878-81 (2d Cir. 2009) (restrictions on disclosure of receipt of national security letters were not narrowly tailored to fulfill the compelling interest of ensuring no harm to national security); *In re Nat’l Sec. Letter*, 930 F. Supp. 2d 1064, 1075-77 (N.D. Cal. 2013) (restrictions on disclosure of national security letters were not narrowly tailored); *Am. Freedom Defense Initiative*, 898 F. Supp. 2d at 83 (granting a preliminary injunction against a prohibition on a pro-Israel and anti-Muslim subway advertisement because it was unnecessary to serve the concededly compelling interest of protecting passenger safety).⁴

The need for such vigilance is if anything even more compelling where, as here, the decision to suppress speech rests entirely in the hands of administrative officials operating purely based on a promise of non-enforcement with no discernible standards governing the exercise of their discretion and no legal framework governing the de facto licensing system they have created. *See City of Lakewood v. Plain Dealer Publ’g Co.*, 486 U.S. 750, 757 (1988) (referring to the “time-tested knowledge that in the area of free expression a licensing statute placing

⁴ The seriousness with which the courts take this requirement is reflected in the strict application of the least restrictive alternative test even to content-based restrictions that impact non-political speech, which occupies a lower “rung on the hierarchy of First Amendment values.” *Alvarez*, 132 S. Ct. at 2551 (the Government failed to show why additional speech or creating a database of Congressional Medal of Honor recipients would not have been viable less restrictive alternatives to a criminal prohibition on false claims to have received the medal); *Am. Civil Liberties Union*, 542 U.S. at 670 (a prohibition on posting material harmful to minors without imposing age-verification procedures violated the First Amendment because it was not narrowly tailored due to the Government’s failure to show that alternatives such as encouraging the use of blocking and filtering software would not be equally as effective); *Playboy Ent. Grp., Inc.*, 529 U.S. at 827 (striking down restrictions designed to prevent “signal bleed” from sexually explicit stations because the Government had failed to show that individual blocking requests were not a viable less restrictive alternative); *Fabulous Assocs., Inc. v. Pa. Pub. Utils. Comm’n*, 896 F.2d 780, 785-88 (3d Cir. 1990) (restrictions on access to providers of sexually explicit telephone messaging services struck down because of availability of other alternatives).

unbridled discretion in the hands of a government official or agency constitutes a prior restraint and may result in censorship”); *see also* *ACLU v. Reno*, 929 F. Supp. 824, 857 (E.D. Pa. 1996) (“[T]he bottom line is that the First Amendment should not be interpreted to require us to entrust the protection it affords to the judgment of prosecutors.”).

As with virtually all such restrictions, the restrictions at issue here – specifically (1) the required reporting of aggregate request data in bands of 1,000 and (2) the prohibition on disclosure of aggregate national security requests received and accounts affected by individual national security authority (e.g., NSL, FISA, or Section 702 of FISA) – fail to meet this demanding standard.⁵ Beginning with the former, the Government’s restriction irrationally prohibits a provider’s disclosure that the provider has received 6,500 requests while permitting the disclosure that the provider has received 6,000-7,000 requests.⁶ There could be no basis for asserting that the first disclosure harms national security while the second does not, and the Government’s brief tellingly makes no effort to defend its restriction. Thus, the Government has not even purported to satisfy its constitutional obligation to determine the least restrictive alternative or impose only those restrictions that are necessary to protect a compelling government interest.

The ban on the providers’ ability to disclose the aggregate number of national security requests that they receive also is unnecessary to protect national security. As indicated above,

⁵ Apple addresses in this brief only the ban on disclosure of the aggregate number of national requests received and the requirement that the aggregate number of law-enforcement requests be grouped in bands of 1,000. It does not address the prohibition on providers’ disclosure of the total number of process received in each FISA category, although it endorses the other providers’ assertion that these prohibitions also are not narrowly tailored.

⁶ To avoid any suggestion that it has disclosed the actual number of requests it has received, Apple is using Microsoft’s reported 6,000-7,000 range to illustrate the point. *See* Microsoft Corporation’s First Amended Motion for Declaratory Judgment or Other Appropriate Relief Authorizing Disclosure of Aggregate Data Regarding Any FISA Orders It Has Received at 4.

Apple has 350 million iCloud customers worldwide and has sold nearly 700 million iPad and iPhone devices in the company's history. There were only 1,000-2,000 combined law-enforcement and national security requests for user account information to Apple in the first half of 2013. *See* Ex. 1 at 3. Whatever percentage of this number is accounted for by national security requests would necessarily represent an infinitesimal fraction of Apple's overall subscriber base. It is therefore simply not possible that disclosure of the aggregate figure could compromise an investigation or reveal to a user that the user has been targeted under FISA or the FISA Amendments Act. *See In re Nat'l Sec. Letter*, 930 F. Supp. 2d at 1076 (observing that the interest in prohibiting disclosure diminishes as a provider's subscriber base increases).

The Government does not appear to argue that disclosing the total number of nondescript FISA process the providers have received would reveal any target-specific data, but asserts nonetheless that this focus is too narrow because the proposed disclosure could enable adversaries to avoid surveillance. Gov't Resp. at 19. This assertion, however, does not withstand scrutiny. It simply is not a secret that the user accounts of some of the largest electronic communications service providers in the world can be and are subject to FISA surveillance. The NSA has publicly admitted that it regularly compels information from service providers. National Security Agency, *The National Security Agency: Missions, Authorities, Oversight and Partnerships*, Lawfare, 6 (Aug. 9, 2013), available at <http://www.lawfareblog.com/wp-content/uploads/2013/10/NSA-August-9-2013-Memorandum-on-Missions-Authorities-Oversight-and-Partnerships.pdf> ("Under all FISA and FAA programs, the government compels one or more providers to assist NSA with the collection of information responsive to the foreign intelligence need."). And the very fact that the providers are filing these motions shows that they receive such process because if they received no such process,

there would be no legal bar to saying so. *See also* Chenda Ngak, *Apple, Microsoft, Facebook Release New Details on National Security Requests*, CBSNews (June 17, 2013), available at http://www.cbsnews.com/8301-205_162-57589619/apple-microsoft-facebook-release-new-details-on-national-security-requests/ (“Facebook and Microsoft say they were granted permission from the U.S. government to disclose more information about FISA requests and national security letters, but only if aggregated with criminal requests from local, state and federal law enforcement.”).

Moreover, by the logic of the Government, the “safest” platforms would be those who receive no FISA requests, but there is no bar to those platforms saying that they have received no FISA requests. Thus, if the Government’s predictions were sound, our adversaries would already know “which platforms the Government *does not* surveil.” Gov’t Resp. at 11. For example, Apple’s November 5 Report on Government Information Requests discloses that “Apple has never received an order under Section 215 of the USA Patriot Act.” Ex. 1 at 5.

There also is no basis for believing that release of the aggregate number of requests received by major providers would reveal anything about the ability to conduct surveillance of those who use these platforms that is not already known. The type of data that these services have and do not have on their servers (whether email, Facebook account information, or something else) is not classified information. It is rather a core element of the services that they provide. For example, Apple’s November 5 report explains that it protects “personal conversations by providing end-to-end encryption over iMessage and FaceTime.” Ex. 1 at 1. The Report further explains that Apple does not “store location data, Maps searches, or Siri requests in any identifiable form.” *Id.* At the same time, Apple users know that they use Apple’s services to store content online, including emails, music, and photographs through such

services as iTunes and iCloud, and that such content may accordingly be the subject of FISA requests as well as requests from state and local law-enforcement agencies.

Further, the basic methods of intelligence gathering that would be the subject of the disclosures also are not classified. Instead, they appear in the pages of the still unclassified United States Code. Given this publicly available information, an adversary who uses Yahoo! (particularly one sophisticated enough to monitor provider disclosures) could not be using Yahoo! because he believes it is immune from surveillance or because he believes Yahoo! is safer than other platforms. Instead, he is using that service because it provides the functionality he needs and because he believes that he has not been targeted for surveillance. The disclosures sought, if allowed, would not disabuse him of either notion.

The foregoing is why it is fundamentally misleading (and perpetuating of the very misconceptions that the providers have filed these motions to correct) for the Government to assert throughout its brief that the Government is subjecting “providers” to surveillance when it, for example, issues a FISA request related to an individual user account. A search of a particular user’s Facebook account is no more surveillance of Facebook than a search warrant executed on a single house is surveillance of the United States. The Government also has imposed the same restrictions on all providers. This one-size-fits-all approach further demonstrates the absence of any basis for the suggestion that the prohibitions are designed to prevent the release of information that would demonstrate that the users of one provider are exceedingly vulnerable to, or uniquely immune from, the reach of the Government.

With respect to particular FISA categories, the Government itself has agreed to report the aggregate numbers of both FISA orders, and the targets those orders affect, on an annual basis. Office of the Director of National Intelligence, *DNI Clapper Directs Annual Release of*

Information Related to Orders Issued Under National Security Authorities, IC on the Record (Aug. 29, 2013), *available at* icontherecord.tumblr.com. Those reports will quantify the number of times the Government has invoked each surveillance “method” authorized by FISA, including the number of FISA orders issued on the basis of probable cause under Sections 703 and 704, Section 702 orders, FISA Pen Register and Trap and Trace Orders under Title IV, business records requests pursuant to Title V, and more. *Id.* These disclosures further demonstrate that disclosure of the relative number of aggregate requests in each category does not harm national security, particularly when, as is the case with the providers that have filed motions as well as Apple, any given request could be targeting any one of hundreds of millions of potential targets.

The Government has also placed on providers the burden of moving for judicial review to lift the speech restrictions rather than imposing a burden on itself to seek judicial review to impose such a requirement. *See Doe*, 549 F.3d at 881 (holding that “in the absence of Government-initiated judicial review,” a statutory restriction on disclosure of the receipt of a national security letter “is not narrowly tailored to conform to First Amendment procedural standards”).

As a final note, Apple notes the Government’s unintentionally revealing statement on page 1 of its brief that “the Government has taken a number of significant steps – above and beyond what the law requires – in order to promote transparency.” It should go without saying that the First Amendment is law. Thus, any disclosures the Government has authorized as unnecessary to protect national security are, by definition, not “above and beyond what the law requires.” They are what the law requires. The Government’s suggestion that permitting speech is a function of grace and dispensation, rather than a constitutional requirement, further

demonstrates that it has not narrowly tailored the restrictions it has placed on the disclosure of aggregate data by providers.

CONCLUSION

For the foregoing reasons, the providers' motions should be granted, and the Court should declare that the providers have a right to disclose accurate information about the number of national security requests received and the number of user accounts affected.

* * *

Pursuant to FISC Rule of Procedure 7(h)(1), Attorneys for *Amicus* Apple Inc. certify that the undersigned attorneys are members in good standing of the Bar of the District of Columbia. Attorneys further certify that they do not currently hold a security clearance.

Dated: November 5, 2013

Respectfully submitted,



William Isaacson, D.C. Bar No. 414788
Samuel C. Kaplan, D.C. Bar No. 463350
Michael J. Gottlieb, D.C. Bar No. 974960
BOIES, SCHILLER & FLEXNER, LLP
5301 Wisconsin Ave. NW
Washington, DC 20015
(t) (202) 237-2727
(f) (202) 237-6131
wisaacson@bsflp.com

Attorneys for *Amicus Curiae* Apple Inc.

CERTIFICATE OF SERVICE

I hereby certify this 5th day of November, 2013, that I caused the foregoing document to be served by hand delivery on the following:

Christine Gunning
Litigation Security Group
United States Department of Justice
2 Constitution Square
145 N St., NE, Suite 2W-115
Washington, DC 20530

In addition, I caused the foregoing document to be served by electronic mail on:


Albert Gidari
Perkins Coie LLP
1201 Third Avenue, Suite 4900
Seattle, WA 98101
agidari@perkinscoie.com
Counsel for Google Inc.

James Garland
Covington & Burling LLP
1201 Pennsylvania Avenue, NW
Washington, DC 20004
jgarland@cov.com
Counsel for Microsoft Corporation

Carl Nichols
Wilmer Cutler Pickering Hale and Dorr LLP
1875 Pennsylvania Avenue, NW
Washington, DC 20006
Carl.nichols@wilmerhale.com
Counsel for Facebook, Inc.

Marc Zwillinger
ZwillGen PLLC
1705 N St. NW
Washington, DC 20036
marc@zwillgen.com
Counsel for Yahoo! Inc.

Jerome C. Roth
Munger, Tolles & Olson LLP
560 Mission Street, 27th Floor
San Francisco, CA 94105
Jermone.Roth@mto.com
Counsel for LinkedIn Corporation



Samuel C. Kaplan

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2013 NOV -5 PM 4:42

LEEANN FLYNN HALL
CLERK OF COURT

Exhibit 1



Report on Government Information Requests

November 5, 2013

We believe that our customers have a right to understand how their personal information is handled, and we consider it our responsibility to provide them with the best privacy protections available. Apple has prepared this report on the requests we receive from governments seeking information about individual users or devices in the interest of transparency for our customers around the world.

This report provides statistics on requests related to customer accounts as well as those related to specific devices. We have reported all the information we are legally allowed to share, and Apple will continue to advocate for greater transparency about the requests we receive.

Protecting Personal Data

Apple offers customers a single, straightforward privacy policy that covers every Apple product. Customer privacy is a consideration from the earliest stages of design for all our products and services. We work hard to deliver the most secure hardware and software in the world, including such innovative security solutions as Find My iPhone and Touch ID, which have made the iPhone both more secure and more convenient.

Perhaps most important, our business does not depend on collecting personal data. We have no interest in amassing personal information about our customers. We protect personal conversations by providing end-to-end encryption over iMessage and FaceTime. We do not store location data, Maps searches, or Siri requests in any identifiable form.

Advocating for Greater Transparency

At the time of this report, the U.S. government does not allow Apple to disclose, except in broad ranges, the number of national security orders, the number of accounts affected by the orders, or whether content, such as emails, was disclosed. We strongly oppose this gag order, and Apple has made the case for relief from these restrictions in meetings and discussions with the White House, the U.S. Attorney General, congressional leaders, and the courts. Despite our extensive efforts in this area, we do not yet have an agreement that we feel adequately addresses our customers' right to know how often and under what circumstances we provide data to law enforcement agencies.

We believe that dialogue and advocacy are the most productive way to bring about a change in these policies, rather than filing a lawsuit against the U.S. government. Concurrent with the release of this report, we have filed an Amicus brief at the Foreign Intelligence Surveillance Court (FISA Court) in support of a group of cases requesting greater transparency. Later this year, we will file a second Amicus brief at the Ninth Circuit in support of a case seeking greater transparency with respect to National Security Letters. We feel strongly that the government should lift the gag order and permit companies to disclose complete and accurate numbers regarding FISA requests and National Security Letters. We will continue to aggressively pursue our ability to be more transparent.

Requests from Law Enforcement

Like many companies, Apple receives requests from law enforcement agencies to provide customer information. As we have explained, any government agency demanding customer content from Apple must get a court order.¹ When we receive such a demand, our legal team carefully reviews the order. If there is any question about the legitimacy or scope of the court order, we challenge it. Only when we are satisfied that the court order is valid and appropriate do we deliver the narrowest possible set of information responsive to the request.

Unlike many other companies dealing with requests for customer data from government agencies, Apple's main business is not about collecting information. As a result, the vast majority of the requests we receive from law enforcement seek information about lost or stolen devices, and are logged as **device requests**. These types of requests frequently arise when our customers ask the police to assist them with a lost or stolen iPhone, or when law enforcement has recovered a shipment of stolen devices.

Only a small fraction of the requests that Apple receives seek personal information related to an iTunes, iCloud, or Game Center account. Account-based requests generally involve account holders' personal data and their use of an online service in which they have an expectation of privacy, such as government requests for customer identifying information, email, stored photographs, or other user content stored online. Apple logs these as **account requests**.

We believe it is important to differentiate these categories and report them individually. Device requests and account requests involve very different types of data. Many of the device requests we receive are initiated by our own customers working together with law enforcement. Device requests never include national security-related requests.

Reporting the Number of Requests for Information About Customer Accounts

The following tables detail the account requests and device requests Apple received from law enforcement agencies between January 1, 2013, and June 30, 2013.

Table 1 shows account requests. The U.S. government has given us permission to share only a limited amount of information about these orders, with the requirement that we combine national security orders with account-based law enforcement requests and report only a consolidated range in increments of 1000.

The most common account requests involve robberies and other crimes or requests from law enforcement officers searching for missing persons or children, finding a kidnapping victim, or hoping to prevent a suicide. Responding to an account request usually involves providing information about an account holder's iTunes or iCloud account, such as a name and an address. In very rare cases, we are asked to provide stored photos or email. We consider these requests very carefully and only provide account content in extremely limited circumstances.

Table 2 shows device requests. Even though device requests have not been the focus of public debate, we are disclosing them to make our report as comprehensive as possible. These may include requests for the customer contact information provided to register a device with Apple or the date the device first used Apple services. We count devices based on the individual serial numbers related to an investigation.

For further information about data in these tables, please see the [glossary](#) below.

¹ National Security Letters (NSLs), which are often the first step in an investigation, do not carry a court order but by law they may not be used to obtain customer content. NSL orders are limited to transactional data such as a customer's contact information. Apple is required by law to comply with these requests if we have the information being sought. Apple assesses the legitimacy of each NSL as if it were a regular court order.

Table 1: Account Information Requests

Country ²	Total Number of Law Enforcement Account Requests Received	Number of Accounts Specified in the Requests	Number of Accounts for Which Data Was Disclosed	Number of Account Requests Where Apple Objected	Number of Account Requests Where Non-Content Data Was Disclosed	Number of Account Requests Where No Data Was Disclosed	Number of Account Requests Where Some Content Was Disclosed	Percentage of Account Requests Where Some Data Was Disclosed
Australia	74	75	41	22	34	40	0	54%
Austria	2	2	1	1	1	1	0	50%
Bahamas	1	1	1	0	0	1	0	100%
Belarus	1	1	0	1	1	0	0	0%
Belgium	13	20	4	8	8	5	0	38%
Brazil	8	8	0	8	8	0	0	0%
Canada	6	6	4	0	2	4	0	67%
China	6	6	2	4	4	2	0	33%
Czech Republic	2	2	1	1	1	1	0	50%
Denmark	11	11	6	5	5	6	0	55%
France	71	72	14	49	54	17	0	24%
Germany	93	93	5	86	87	6	0	6%
Hong Kong	32	33	25	4	8	24	0	75%
Ireland	5	5	3	2	2	3	0	60%
Italy	60	76	18	34	38	22	0	37%
Japan	42	49	3	21	32	10	0	24%
Netherlands	4	4	1	3	3	1	0	25%
New Zealand	3	3	1	2	2	1	0	33%
Norway	6	6	2	4	4	2	0	33%
Poland	1	2	0	1	1	0	0	0%
Portugal	2	2	2	0	0	0	0	100%
Russia	1	1	1	0	0	1	0	100%
San Marino	2	2	0	2	2	0	0	0%
Singapore	23	23	13	9	10	13	0	57%
South Korea	4	4	2	2	2	2	0	50%
Spain	102	104	19	77	80	22	0	22%
Sweden	7	7	3	3	4	3	0	43%
Switzerland	6	6	1	4	5	1	0	17%
Taiwan	4	4	1	1	1	3	0	75%
United Kingdom	127	141	51	79	80	46	1	37%
United States	1000-2000	2000-3000	0-1000	0-1000	0-1000	0-1000	0-1000	—

² Personal information regarding individuals who reside in a member state of the European Economic Area (EEA) is controlled by Apple Distribution International in Cork, Ireland, and processed on its behalf by Apple Inc. Personal information collected in the EEA when using iTunes is controlled by iTunes SARL in Luxembourg and processed on its behalf by Apple Inc. All personally identifiable content is hosted on servers within the United States. Accordingly, law enforcement agencies outside the United States seeking such content must obtain legal process through U.S. authorities. Where the foreign country has signed a Mutual Legal Assistance Treaty (MLAT) with the United States, then appropriate legal process can be obtained through the process specified in the treaty or through other cooperative efforts with the U.S. Department of Justice.

Table 2: Device Information Requests

Country ²	Total Number of Law Enforcement Device Requests Received	Number of Devices Specified in the Requests	Number of Device Requests Where Some Data Was Provided	Percentage of Device Requests Where Some Data Was Provided
Australia	1178	1929	695	59%
Austria	49	104	39	80%
Bahamas	1	1	1	100%
Belgium	64	175	41	64%
Brazil ³	34	5057	2	6%
Canada	38	224	35	92%
Chile	1	1	1	0%
China	585	1268	429	73%
Cyprus	1	1	0	0%
Czech Republic	12	99	7	58%
Denmark	55	132	41	75%
Estonia	1	1	0	0%
Finland	3	4	2	67%
France	530	2679	334	63%
Germany	2156	4928	1856	86%
Greece	2	8	2	100%
Hong Kong	92	267	64	70%
Hungary	12	13	3	25%
India	27	65	11	41%
Ireland	102	379	79	77%
Italy	409	4034	331	81%
Japan	106	182	12	11%
Luxembourg	67	92	29	43%
Malaysia	1	2	0	0%
Netherlands	61	229	40	66%
New Zealand	71	116	42	59%
Norway	33	101	27	82%
Poland	2	53	1	50%
Portugal	17	300	14	82%
Russia	13	15	12	92%
Singapore	1498	1681	853	57%
Slovenia	4	5	2	50%
South Korea	88	419	46	52%
Spain	308	463	244	79%
Swaziland	1	1	0	0%
Sweden	61	102	54	89%
Switzerland	107	139	91	85%
Taiwan	81	115	10	12%
United Arab Emirates	1	1	1	100%
United Kingdom	1028	2474	689	67%
United States	3542	8605	3110	88%

² Personal information regarding individuals who reside in a member state of the European Economic Area (EEA) is controlled by Apple Distribution International in Cork, Ireland, and processed on its behalf by Apple Inc. Personal information collected in the EEA when using iTunes is controlled by iTunes SARL in Luxembourg and processed on its behalf by Apple Inc. All personally identifiable content is hosted on servers within the United States. Accordingly, law enforcement agencies outside the United States seeking such content must obtain legal process through U.S. authorities. Where the foreign country has signed a Mutual Legal Assistance Treaty (MLAT) with the United States, then appropriate legal process can be obtained through the process specified in the treaty or through other cooperative efforts with the U.S. Department of Justice.

³ Five requests are related to the recovery of stolen cargoes of devices.

Notes

Apple keeps track of every request we receive. Some countries are not listed in this report because Apple has not received any information requests from the government there.

The number of affected accounts and devices is often larger than the number of requests because law enforcement may seek information related to multiple accounts or devices. For example, some device requests related to the theft of a shipment may involve hundreds of serial numbers.

In cases where no data was disclosed, Apple may have objected to a government request for legal reasons or searched our records and discovered that we have no relevant information. This category includes multiple scenarios in which no data was disclosed.

Apple has never received an order under Section 215 of the USA Patriot Act. We would expect to challenge such an order if served on us.

Glossary of Terms

Table 1 Definitions

Total Number of Law Enforcement Account Requests Received

The total number of account-based requests issued by a government agency and/or a court that are received by Apple and seek customer data related to specific Apple IDs, email addresses, telephone numbers, credit card numbers, or other personal identifiers. Account-based law enforcement requests come in various forms such as subpoenas, court orders, and warrants.

Number of Accounts Specified in the Requests

The number of discernible accounts, based on specific Apple IDs, email addresses, telephone numbers, credit card numbers, or other personal identifiers in each law enforcement request. A single request may involve multiple accounts where, for example, multiple accounts are associated with the same credit card.

Number of Accounts for Which Data Was Disclosed

The number of discernible accounts, based on specific Apple IDs, email addresses, telephone numbers, credit card numbers, or other personal identifiers, for which Apple provided some iCloud, iTunes, or Game Center data.

Number of Account Requests Where Apple Objected

The number of law enforcement requests that resulted in Apple refusing to provide some data based on various grounds, such as jurisdiction, improper process, insufficient process, invalid process, or where the scope of the request was excessively broad. For example, Apple may object to a law enforcement request as "invalid" if it was not signed.

Number of Account Requests Where Non-Content Data Was Disclosed

The number of law enforcement requests that resulted in Apple providing only subscriber or transactional information, but not content. For example, Apple may provide subscriber information and a limited purchase history in response to valid legal process.

Number of Account Requests Where No Data Was Disclosed

The number of law enforcement requests that resulted in Apple providing no customer information whatsoever.

Number of Account Requests Where Some Content Was Disclosed

The number of law enforcement requests where Apple determined that an account request was lawful and provided content such as iCloud email, contacts, calendar, or Photo Stream content. Apple only provides user account content in extremely limited circumstances.

Percentage of Account Requests Where Some Data Was Disclosed

The percentage of law enforcement requests that resulted in Apple providing some iCloud, iTunes, or Game Center data.

Table 2 Definitions

Total Number of Law Enforcement Device Requests Received

The number of device-based requests issued by a government agency and/or a court that are received by Apple and seek customer data related to specific device identifiers such as serial or IMEI numbers. Law enforcement device requests come in various forms such as subpoenas, court orders, and warrants. A single request may involve multiple devices. For example, in the case of a recovered shipment of stolen devices, law enforcement may seek information related to several devices in a single request.

Number of Devices Specified in the Requests

The total number of iPhone, iPad, iPod, Mac, or other devices identified in each law enforcement request, based on the number of device identifiers. For example, law enforcement agencies investigating theft cases often send requests seeking information based on serial numbers. Each serial number is counted as a single device. A request may involve multiple devices as in the case of a recovered shipment of stolen devices.

Number of Device Requests Where Some Data Was Provided

The number of law enforcement requests that resulted in Apple providing relevant device information, such as registration, subscriber, service, repair, and purchase information in response to valid legal process.

Percentage of Device Requests Where Some Data Was Provided

The percentage of law enforcement requests that resulted in Apple providing some relevant device information in response to valid legal process.

U.S. FOREIGN
INTELLIGENCE
SURVEILLANCE COURT

2013 NOV -5 PM 4:42

LEEANN FLYNN HALL
CLERK OF COURT

Exhibit 2



U.S. Department of Justice
Federal Bureau of Investigation

Washington, D. C. 20535-0001

June 17, 2013

Jane C. Horvath
Director of Global Privacy
1 Infinite Loop
Cupertino, CA 90514

Dear Ms. Horvath:

We appreciate your discussion with us about your proposal to disclose certain information about the volume of legal process Apple receives.

As we discussed during our phone call on June 15, 2013, we do not intend to seek enforcement¹ of the non-disclosure provisions associated with any legal process, including FISA orders, in connection with the aggregate data described below, so long as Apple aggregates data for all of the legal process it received for intervals of six months, beginning with the period ending May 31, 2013, from any and all government entities in the United States (including local, state, and federal, and including criminal and national security-related requests) into bands of 1000, starting at zero, and which you may break down into one or both of the following two categories: the number of requests and the number of user accounts for which data was requested.

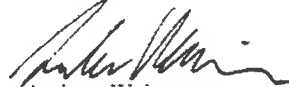
This position is an exercise of FBI discretion in light of current circumstances and the precise contours of this letter. Accordingly, our decision does not reflect the FBI's position with respect to potential disclosures by Apple that differ in any respect from the disclosures outlined in this letter. Nor is our decision a precedent for disclosures by any other company that is in receipt of such process, even if the disclosures were made in the manner that is proposed in this letter. The national security implications of disclosures related to the receipt of such process may vary depending on the identity of the company that is making the disclosure and the overall number of disclosures by different companies. For this reason, if other companies also seek to disclose information about the volume of such process that they receive, that may alter our calculus about the implications of disclosures by Apple. In addition, our current determination is based on our prediction about the potential national security consequences of the disclosures and as such we may in the future revise our position as circumstances change or as we evaluate the actual impact of your disclosures on national security.

¹ The FBI does not have the authority to negate a court order, nor can we bind state or local authorities.

This letter further commits Apple to coordinate with us before making any additional public disclosures about the volume of legal process you receive, beyond the contours outlined in this letter. If we revise our position, we will notify you. We would retain the right to bring an appropriate enforcement action with respect to any future disclosures you make after you receive a notification of our change in position.

Thank you again for coordinating your proposal with us. We appreciate your efforts to reach an agreement that promotes transparency without jeopardizing our national security responsibilities to the public.

Sincerely,



Andrew Weissmann
General Counsel